<table>
<tr><td colspan="4">UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231</td></tr>
</table>

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
09/224,918	01/04/99	HUNNICUTT	H 1001/028C

WM51/1102

KIRK D WILLIAMS
DUFT GRAZIANO & FOREST
SUITE 140
1790 30TH STREET
BOULDER CO 80301-1018

EXAMINER	
EDELMAN, B	
ART UNIT	PAPER NUMBER
2153	

DATE MAILED: 11/02/00

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner of Patents and Trademarks

☒ Responsive to communication(s) filed on _Sep 6, 2000_

☒ This action is **FINAL.**

☐ Since this application is in condition for allowance except for formal matters, **prosecution as to the merits is closed** in accordance with the practice under *Ex parte Quayle* 1935 C.D. 11; 453 O.G. 213.

A shortened statutory period for response to this action is set to expire _____3___ month(s), or thirty days, whichever is longer, from the mailing date of this communication. Failure to respond within the period for response will cause the application to become abandoned. (35 U.S.C. § 133). Extensions of time may be obtained under the provisions of 37 CFR 1.136(a).

Disposition of Claim

☒ Claim(s) _1, 3-5, 7-15, and 17-33_ is/are pending in the applicat

   Of the above, claim(s) _____ is/are withdrawn from consideration

☐ Claim(s) _____ is/are allowed.

☒ Claim(s) _1, 3-5, 7-15, and 17-33_ is/are rejected.

☐ Claim(s) _____ is/are objected to.

☐ Claims _____ are subject to restriction or election requirement.

Application Papers

☐ See the attached Notice of Draftsperson's Patent Drawing Review, PTO-948.

☐ The drawing(s) filed on _____ is/are objected to by the Examiner.

☐ The proposed drawing correction, filed on _____ is ☐ approved ☐ disapproved.

☐ The specification is objected to by the Examiner.

☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. § 119

☐ Acknowledgement is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d).

   ☐ All ☐ Some* ☒ None of the CERTIFIED copies of the priority documents have been

   ☐ received.

   ☐ received in Application No. (Series Code/Serial Number) _____ .

   ☐ received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   *Certified copies not received: _____

☐ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. § 119(e).

Attachment(s)

☐ Notice of References Cited, PTO-892

☐ Information Disclosure Statement(s), PTO-1449, Paper No(s). _____

☐ Interview Summary, PTO-413

☐ Notice of Draftsperson's Patent Drawing Review, PTO-948

☐ Notice of Informal Patent Application, PTO-152

--- SEE OFFICE ACTION ON THE FOLLOWING PAGES ---

DETAILED ACTION

This action is in response to Applicant's amendment and reconsideration filed on September 8, 2000. Claims 1, 3-5, 7-15, and 17-33 are presented for further examination.

Claim Rejections - 35 USC § 102

1.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless --
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371© of this title before the invention thereof by the applicant for patent.

2.   Claims 1, 7-9, 14-15, 21-23, and 28-31 are rejected under 35 U.S.C. 102(e) as being anticipated by Ensor et al. (U.S. Patent No. 5,721,780, hereinafter "Ensor").

In considering claims 1, 15, and 31, Ensor discloses a system for a computer-implemented method, comprising:

checking a first memory (126) to determine if a user has previously accessed a resource on a computer network (col. 5, lines 10-12, 54-60; note: previous access is determined according to whether or not memory 126 returns a password - see col. 5, lines 54-58) upon receipt of an indication from the user to access the resource (col. 2, lines 43-47); and

providing the user with access to the resource if the first memory indicates that the user

has previously accessed the resource (col. 6, lines 1-6; note: according to Ensor, provision of

access only occurs if that password matches a submitted password (col. 6, lines 1-3). While this

step may seem to impose a further limitation over the claim, thus rendering it different from the

claimed invention, the step is intended to ensure that only users who have authentically gained

previous access can obtain subsequent access. Therefore, while the cited passage includes an

extra authentication step, it still encompasses all steps of the present limitation).

In considering claims 7 and 21, Ensor further discloses the resource being a file (col. 6,

lines 3-5).

In considering claims 8 and 22, Ensor further discloses the resource being volume of files

(col. 3, lines 30-31; wherein "databases" is a volume of files).

In considering claims 9 and 23, Ensor further discloses the resource being a memory

device (col. 3, lines 30-31).

In considering claims 14 and 28, Ensor further discloses the request from the user

indicating an operation to perform with respect to the resource (col. 6, line 5, wherein

"downloading requested software" comprises indicating an operation to perform with respect to the resource) including:

checking the first memory to determine if the user may perform the operation with respect to the resource (col. 5, lines 54-60; the user may perform the operation if the first memory indicates that the user is authorized to access the resource);

checking a second memory (112) to determine if the user may perform the operation with respect to the resource if the first memory does not indicate that the user may perform the operation with respect to the resource (col. 5, lines 8-17);

providing the user with access to the resource if the second memory indicates that the user may perform the operation with respect to the resource (col. 5, lines 22-27, 32-35; if no password match is found in the second memory, then the user may perform the operation with respect to the resource); and

storing information in the first memory indicating that the user may perform the operation with respect to the resource if, after checking the second memory, the second memory indicates that the user may perform the operation with respect to the resource (col. 5, lines 27-32).

In considering claims 29 and 30, Ensor further discloses:

checking a second memory (112) to determine if the user may access the resource if the first memory does not indicate that the user has previously accessed the resource (col. 5, lines 8-17);

providing the user with access to the resource if the second memory indicates that the user

may access the requested resource (col. 5, lines 22-27, 32-35; if no password match is found in

the second memory, then the user may access the resource); and

storing information in the first memory indicating that the user may access the resource if,

after checking the second memory, the second memory indicates that the user may access the

requested resource (col. 5, lines 27-32).

Claim Rejections - 35 USC § 103

3.   Claims 3-4, 10-13, 17-18, 24-27, and 32-33 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Ensor.

In considering claims 3 and 17, although the system taught by Ensor discloses substantial

features of the claimed invention, it fails to explicitly disclose representing the user in the first

memory by a token. However, the system taught by Ensor does disclose representing the user

with a password, and a person having ordinary skill in the art would have readily recognized that a

token is merely one possible representation of a password. Thus it would have been obvious to

use a token as the password to represent the user in the network access system taught by Ensor,

so that the password could have a predictable, set amount of bits.

In considering claims 4 and 18, Ensor further discloses the password, (which could be a

token, as discussed above) also representing a plurality of other users (col. 6, lines 10-16).

In considering claims 10 and 24, although the system taught by Ensor discloses substantial features of the claimed invention, it fails to explicitly disclose storing of the information in the first memory comprising overwriting other information associated with the resource in the first memory. Nonetheless, it is well known in a network resource access system that information relating to access rights can be overwritten if access rights to the system should change. Further, Ensor discloses the possibility that information stored in the first memory could be tampered with, thus causing authentication problems within the network (col. 5, lines 60-65). Therefore, given the likelihood of tampering, it would have been obvious to a person having ordinary skill in the art to overwrite the tampered information with correct information submitted from the users to remedy the faulty authentication situation.

In considering claims 12 and 26, although the system taught by Ensor discloses substantial features of the claimed invention, it fails to disclose removing indications from the first memory allowing access to the resource if the resource is altered. Nonetheless, removing access privileges to a resource after changes have occurred in a network is well known. Thus, it would have been obvious to a person having ordinary skill in the art to remove indications allowing access to the resource, in case the resource is altered to include classified information which should not be viewed by current users.

In considering claims 13 and 27, although the system taught by Ensor discloses substantial features of the claimed invention, it fails to disclose removing indications from the first memory allowing access to the resource if rights to the user are altered. Nonetheless, removing user access privileges to a resource in a network is well known. Thus, it would have been obvious to a person having ordinary skill in the art to remove indications allowing access to the resource in case a user who acts irresponsibly or who changes jobs should no longer have access to classified information.

4.   Claims 5, 19, and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ensor in view of Teper et al. (U.S. Patent no. 5,815,665, hereinafter "Teper").

In considering claims 5 and 19, although the system taught by Ensor discloses substantial features of the claimed invention, it fails to disclose the tokens representing anonymous users. Nonetheless, representing anonymous users with tokens in a network user access system is well known, as evidenced by Teper. In a similar art, Teper discloses a network user access system wherein a token in a first memory ("security system 64C") is checked to determine whether users are allowed access to a system (col. 15, lines 35-51) and wherein the tokens represent anonymous users (col. 5, lines 33-37; col. 6, lines 42-44). A person having ordinary skill in the art would have readily recognized the desirability and advantages of representing users of the system taught by Ensor, anonymously, as taught by Teper, in order to protect user identities by allowing anonymous use over a completely untrusted public network such as the Internet (see Teper, col.

7, lines 2-3). Therefore, it would have been obvious to allow anonymous user access, as taught

by Teper in the user resource access system taught by Ensor.

In considering claim 20, Teper further discloses authorizing the user by checking a

password provided by the user, and associating the token with the user after authorizing the user

(col. 15, lines 21-45). Teper then further discloses using the token to check a memory area for

access rights (col. 15, lines 41-42). It would have been obvious to a person having ordinary skill

in the art to include a password for authorization *in addition to* a token for access rights, as

taught by Teper, instead of using only a *single* password (or token) signifying both authorization

and access rights, as taught by Ensor, because having two separate security measures decreases

the likelihood of unauthorized access by keeping usernames and passwords unknown to the

resource being requested (see Teper - Abstract).

5.   Claims 11 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ensor,

in view of Brown et al. (U.S. Patent No. 5,941,947, hereinafter "Brown").

In considering claims 11 and 25, although the system taught by Ensor discloses substantial

features of the claimed invention, it fails to disclose writing a token for the user in the first

memory over another token for another user that had last previous access to the resource.

Nonetheless, overwriting information related to access rights in a network system is well known,

as evidenced by Brown. In a similar art, Brown describes a network access control system,

wherein access rights to network resources are stored in a cache, and wherein a machine

containing access rights cache contains cache flushing structures which monitor certain activities

to determine when a user-specific access rights list may be overwritten in the cache (col. 28, lines

46-50). Furthermore, the system taught by Brown also describes one method of overwriting data

in the cache including a least-recently-used monitor to determine which access rights to overwrite

(col. 28, lines 50-57). Although the method disclosed by Brown cites a least-recently-used cache

dump, while the claimed invention discloses a last-previously-accessed overwriting process, the

use of any time-dependent access-rights replacement algorithm would have been an obvious

modification to the system taught by Ensor in order to open up storage space in the access-rights

memory in case the memory has become full.

6.   Claims 32-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ensor, in

view of the admitted prior art.

        In considering claim 32, although the system taught by Ensor discloses substantial features

of the claimed invention, it fails to disclose opening the requested resource to determine if the

user may access the requested resource if the memory does not indicate that the user has

previously accessed the resource, and providing the user with access to the requested resource if

the requested resource indicates that the user may access the requested resource. Nonetheless,

the step of opening a requested resource to determine if a user may access the resource, and

providing the user with access to the requested resource if the resource indicates that the user

may access the resource is well known, as admitted in the "statement of the problem" section of

the present application (see page 2, line 30 - page 3, line 5). A person having ordinary skill in the

art would have readily recognized the desirability and advantages of instead of determining

authentication by accessing the service bureau's internal database (112) after first checking a first

memory (126) as taught by Ensor, determining authentication by directly accessing and opening

the resource, as is admittedly well known, after first checking the first memory, as taught by

Ensor, because although the latter method of opening the resource may consume a great deal of

CPU time, as admitted in the specification, it is a more direct method that avoids the necessity of

employing an extra "middle-ware" device.

In considering claim 33, Ensor further discloses storing information in the memory

indicating that the user has previously accessed the requested resource (col. 5, lines 54-60).

Response to Arguments

In response to Applicant's amendment and request for reconsideration filed on September

8, 2000, the following factual arguments are noted:

a)   In considering claims 1, 15, and 31, the claimed invention merely accesses a memory to

determine whether the resource has been previously accessed by the user, and if so, provides

subsequent access. Thus by interrogating the client for a password and authenticating the

password before providing access to requested resources, even if the user has previously accessed

the resource, Ensor does not teach each and every element of the claimed invention.

b)   There is no provision for a single token to represent multiple parties in the Ensor

reference, and thus the Ensor reference cannot fairly be read as suggesting the use of tokens in

general, or the use of a single token by multiple users in particular.

In considering (a), Applicant contends that in considering claims 1, 15, and 31, the

claimed invention merely accesses a memory to determine whether the resource has been

previously accessed by the user, and if so, provides subsequent access. Thus by interrogating the

client for a password and authenticating the password before providing access to requested

resources, even if the user has previously accessed the resource, Ensor does not teach each and

every element of the claimed invention. Examiner respectfully disagrees.

In response, it is necessary to better clarify the process described in cols. 4-5 of Ensor. As

described in columns 4-5, the following steps are disclosed (note that not all steps described by

Ensor are included below - only those that pertain to the present invention are discussed):

I)   A subscriber at a terminal device (110) requests connection to a service bureau (108) -

col. 4, lines 40-50.

II)   A first memory (126) is checked - col. 5, lines 8-12.

III)   If a password is returned from the memory, and the password is authentic, the terminal has

already been previously registered with the service bureau - col. 5, lines 54-58.

IV)   After the password is returned from the memory, the terminal's request is fulfilled - col. 5,

lines 32-35.

According to this process, the existence of a password in the memory signifies that the

terminal has previously accessed the resource (i.e. registered with the service bureau), so long as

the password has not been tampered with or otherwise altered (col. 5, lines 27-32, 60-66).

Further, when the memory indicates that the user has gained previous access (i.e. a password

exists in the memory), the user is provided access to the resource, so long as the password has not

been tampered with or otherwise altered. Thus Ensor goes one step further than the claimed

invention in not only describing that a memory is checked to determine of a user has previously

accessed a resource, but also explaining *how* the checking of the memory determines whether a

user has previously accessed a resource (i.e. checking for a stored password). Although the

claimed invention includes no mention of passwords or authentication, the claimed invention, as

broadly interpreted, is anticipated by the Ensor reference. Therefore, claims 1, 15, and 31 remain

rejected.

In considering (b), Applicant contends that there is no provision for a single token to

represent multiple parties in the Ensor reference, and thus the Ensor reference cannot fairly be

read as suggesting the use of tokens in general, or the use of a single token by multiple users in

particular, as claimed in certain ones of claims 3-5, 11, 17, 18, and 25. Examiner respectfully

disagrees.

As suggested by Applicant in Applicant's most recent response, filed on September 8,

2000, "in general, a password may be represented as a token". Examiner has recognized this and

had rejected the original claims in view of this fact, and with the reasoning that it would have been

obvious to use a token to represent the password representing the user in the network access

system taught by Ensor, so that the password could have a predictable, set amount of bits.

Furthermore, Ensor further discloses the password (i.e. token) representing a plurality of users

(col. 6, lines 10-16). Although the individual passwords of each user may be unique, the portion

which is evaluated for access purposes is effectively the same - (col. 6, lines 13-14, "only portions

of the passwords actually match"). Thus, a portion of the password used for access purposes

(which can be implemented as a token as discussed above) in the system described by Ensor

represents a plurality of users. Therefore, the claims pertinent to this argument remain rejected.

Conclusion

7.   **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time

policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within TWO

MONTHS of the mailing date of this final action and the advisory action is not mailed until after

the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.
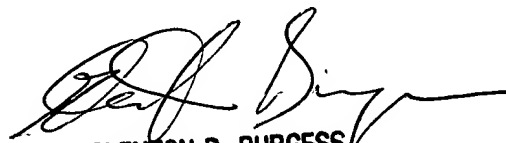
8.   Any inquiry concerning this communication or earlier communications from the examiner should be directed to Bradley Edelman whose telephone number is (703) 306-3041. The examiner can normally be reached on Monday to Friday from 8:30 AM to 5:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Glen Burgess, can be reached on (703) 305-4792. The fax phone number for the organization where this application or proceeding is assigned is (703) 305-7201.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 308-3900.

GLENTON B. BURGESS
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

BE

October 27, 2000